在Windows上安装安全终端所需的根证书列表故障排除

目录

简介

本文档介绍如何检查高级恶意软件防护(AMP)安装因证书错误而失败时安装的所有证书颁发机构。

使用的组件

- 安全连接器（以前称为面向终端的AMP）6.3.1或更高版本
- 从Windows 7开始

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题

如果您遇到面向终端的AMP for Endpoints Connector for Windows的问题，请检查此位置下的日志。

<#root>

```
C:\ProgramData\Cisco\AMP\immpro_install.log
```

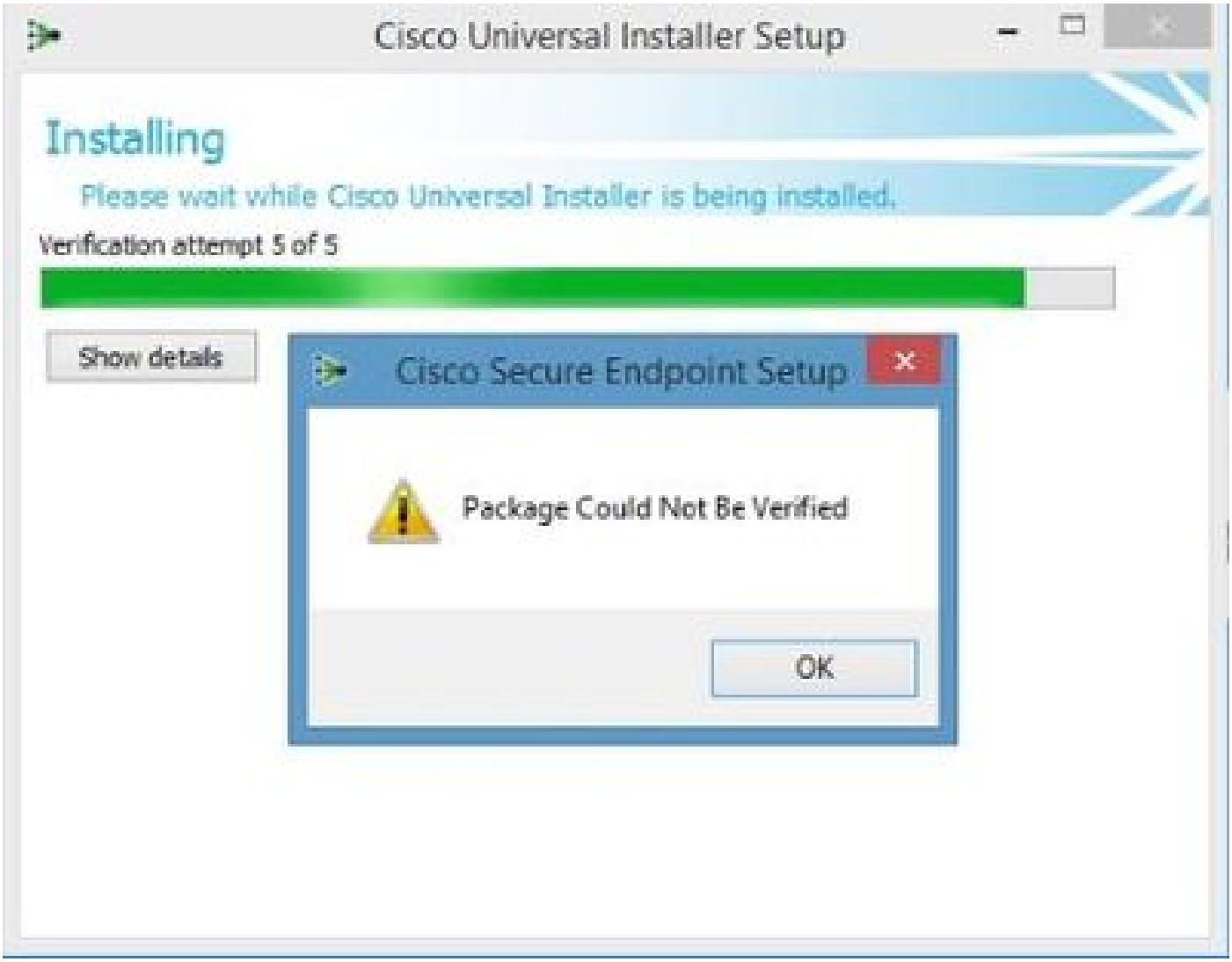
如果您看到此消息或类似的消息。

<#root>

```
ERROR: Util::VerifyAll: signature verification failed : -2146762487 : A certificate chain processed, but
```

<#root>

```
Package could not be verified
```



确保已安装所有必要的RootCA证书。

解决方案

步骤1:使用管理权限打开PowerShell并运行命令。

<#root>

```
Get-ChildItem -Path Cert:LocalMachine\Root
```

结果显示计算机上存储的已安装RootCA证书的列表。

第二步：将步骤1中获得的指纹与下表1中列出的指纹进行比较：

指纹	主题名称/属性
3B1EFD3A66EA28B16697394703A72CA340A05BD5	CN=Microsoft Root Certificate Authority 2010, O=Microsoft Corporation，

	L=Redmond， S=Washington， C=US
D69B561148F01C77C54578C10926DF5B856976AD	CN=GlobalSign， O=GlobalSign，OU=GlobalSign根CA - R3
D4DE20D05E66FC53FE1A50882C78DB2852CAE474	CN=Baltimore CyberTrust Root、OU=CyberTrust、O=Baltimore、C=IE
D1EB23A46D17D68FD92564C2F1F1601764D8E349	CN=AAA Certificate Services、O=Comodo CA Limited、L=Salford、S=Greater Manchester、C=GB
B1BC968BD4F49D622AA89A81F2150152A41D829C	CN=GlobalSign Root CA、OU=Root CA、O=GlobalSign nv-sa、C=BE
AD7E1C28B064EF8F6003402014C3D0E3370EB58A	OU=Starfield Class 2认证机构，O="Starfield Technologies，Inc.",C=US
A8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436	CN=DigiCert Global Root CA，OU=www.digicert.com, O=DigiCert Inc， C=US
742C3192E607E424EB4549542BE1BBC53E6174E2	OU=Class 3 Public Primary Certification Authority， O="VeriSign， Inc.", C=US
5FB7EE0633E259DBAD0C4C9AE6D38F1A61C7DC25	CN=DigiCert High Assurance EV Root CA， OU=www.digicert.com, O=DigiCert Inc， C=US
4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c)2006 VeriSign， Inc. — 仅供授权使用", OU=VeriSign Trust Network，O="VeriSign， Inc.", C=US
2796BAE63F1801E277261BA0D77770028F20EEE4	OU=Go Daddy 2级认证机构，O="The Go Daddy Group， Inc.",C=US
0563B8630D62D75ABBC8AB1E4BDFB5A899B24D43	CN=DigiCert Assured ID Root CA，OU=www.digicert.com, O=DigiCert Inc， C=US
DDFB16CD4931C973A2037D3FC83A4D7D775D05E4	CN=DigiCert Trusted Root G4, OU=www.digicert.com, O=DigiCert Inc， C=US
CA3AFBCF1240364B44B216208880483919937CF7	CN=QuoVadis Root CA 2, O=QuoVadis Limited， C=BM
2B8F1B57330DBBA2D07A6C51F70EE90DDAB9AD8E	CN=USERTrust RSA Certification Authority， O=USERTRUST Network，L=泽西市， S=新泽西， C=US
F40042E2E5F7E8EF8189FED15519AECE42C3BFA2	CN=Microsoft Identity Verification Root Certificate Authority 2020, O=Microsoft Corporation， L=Redmond，S=Washington， C=US

DF717EAA4AD94EC9558499602D48DE5FBCF03A25	CN=US， O=IdenTrust， CN=IdenTrust商业根CA 1

表 1.Cisco Secure Connector所需的证书列表。

第三步：从PEM格式的发行者下载计算机存储中不存在的证书。

提示：您可以通过Internet上的指纹搜索证书。它们唯一地定义证书。

第四步：从“开始”菜单打开mmc控制台。

第五步：导航到文件>添加/删除管理单元…… >证书>添加>计算机帐户>下一步>完成>确定。

第六步：在受信任的根证书颁发机构下打开证书。右键单击Certificates文件夹，然后选择All Tasks > Import...并按照向导操作以导入证书，直到证书出现在Certificates文件夹中。

步骤 7.如果要导入更多证书，请重复步骤6。

步骤 8导入所有证书后，检查面向终端的AMP连接器安装是否成功。如果不是，请再次检查immpro_install.log文件中的日志。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。